BA

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－22680
（P2000－22680A）
(43)公開日　平成12年１月21日(2000.1.21)

(51)Int.Cl.⁷		識別記号	FI		テーマコード（参考）
H04L	9/08		H04L	9/00	601B
G06F	15/00	330	G06F	15/00	330Z
	17/60		G09C	1/00	620Z
G09C	1/00	620			640C
		640	G06F	15/21	330

審査請求　未請求　請求項の数７　ＯＬ　（全 11 頁）

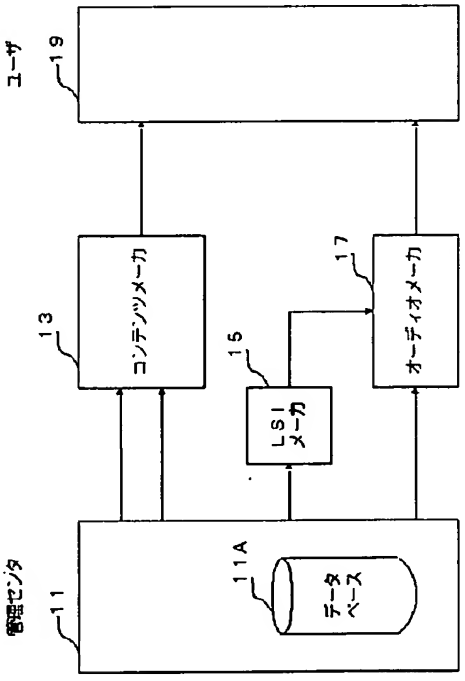
(21)出願番号　特願平10－191706

(22)出願日　平成10年７月７日(1998.7.7)

(71)出願人　598090519
株式会社オープンループ
北海道札幌市清田区清田七条一丁目18番５号
(72)発明者　浅田　一嶽
北海道札幌市清田区北野７条２丁目５番５号　株式会社オープンループ内
(74)代理人　100095407
弁理士　木村　満　（外２名）

(54)【発明の名称】　ディジタルコンテンツ流通方法及びコンテンツを再生可能に記録した記録媒体

(57)【要約】
【課題】　音楽等のディジタルコンテンツの不正コピー利用を防止し、安全に流通させる。
【解決手段】　管理センタ１１は、マスタ公開鍵KPUkをコンテンツメーカに供給し、マスタープライベート鍵KPRkをＬＳＩメーカ１５に供給する。コンテンツメーカ１３は、コンテンツ別にコンテンツ暗号鍵Kcoを生成して暗号化したデータと、コンテンツ暗号鍵Kcoをマスタ公開鍵KPUkにより暗号化したデータと、自己の署名と、管理センタ１１からの証明書ＤＶとを記録媒体２１に記録する。ＬＳＩメーカ１５は、暗号化されたコンテンツ暗号鍵を復号するためのマスタープライベート鍵KPRkを復号ＬＳＩに含める。復号機器は、復号ＬＳＩにより、装着された記録媒体２１の証明書ＤＶと署名ＤＳが共に有効であると判断した際に、マスタープライベート鍵KPRkによりコンテンツ暗号鍵を復号し、コンテンツを復号する。



【特許請求の範囲】
【請求項１】ディジタルコンテンツの流通を管理する管理センタと、前記管理センタの管理下に、ディジタルコンテンツを暗号化して流通させるコンテンツメーカと、前記コンテンツメーカが提供するコンテンツを復号して利用可能とする復号手段を提供する復号手段提供手段と、を備える流通システムを用いてディジタルコンテンツを流通する方法であって、
前記コンテンツメーカは、コンテンツ別に生成されたコンテンツ暗号鍵によりコンテンツを暗号化し、
前記管理センタは、暗号化されたコンテンツ暗号鍵を記録媒体に記録するための情報をコンテンツメーカに提供し、
前記コンテンツメーカは、コンテンツ暗号鍵により暗号化されたコンテンツと、暗号化されたコンテンツ暗号鍵とを記録媒体に記録して流通させ、
前記管理センタは、暗号化されたコンテンツ暗号鍵を復号するための復号情報を復号手段提供手段に提供し、
前記復号手段提供手段は、前記暗号化されたコンテンツ暗号鍵を復号するための復号情報を前記復号手段に含め、
前記復号手段は、前記記録媒体に記録されているコンテンツ暗号鍵を前記復号情報を用いて復号し、復号した暗号鍵で、コンテンツを復号して再生する、
ことを特徴とするディジタルコンテンツ流通方法。
【請求項２】前記コンテンツメーカは、コンテンツ別にコンテンツ暗号鍵を生成してコンテンツを暗号化し、生成したコンテンツ暗号鍵を管理センタから供給されたマスタ公開鍵により暗号化し、管理センタから供給された署名用コンテンツメーカプライベート鍵を用いて自己の署名を作成し、暗号化したコンテンツと暗号化したコンテンツ暗号鍵と署名と管理センタから供給された証明書とを記録媒体に格納し、
前記復号手段提供手段は、前記復号手段に、暗号化されたコンテンツ暗号鍵を復号するためのマスタプライベート鍵と、証明書を検証するための署名用センタ公開鍵とを含め、
前記復号手段は、証明書を署名用センタ公開鍵を用いて検証することにより、コンテンツメーカの署名用コンテンツメーカ公開鍵を得て、これにより署名を検証し、証明書及び署名が共に有効であると判断した際に、前記マスタプライベート鍵により暗号化コンテンツ暗号鍵を復号し、復号したコンテンツ暗号化鍵により、コンテンツを復号し、
前記管理センタは、マスタ公開鍵と、コンテンツメーカの署名用コンテンツメーカ公開鍵を署名用センタプライベート鍵で暗号化した情報を含む証明書とをコンテンツメーカに供給し、マスタプライベート鍵と署名用センタ公開鍵を前記復号手段提供手段に供給する、
ことを特徴とする請求項１に記載のディジタルコンテンツ流通方法。
【請求項３】前記コンテンツメーカは、コンテンツ別にコンテンツ暗号鍵を生成してコンテンツを暗号化し、生成したコンテンツ暗号鍵を管理センタに供給し、管理センタから供給された署名用コンテンツメーカプライベート鍵を用いて自己の署名を作成し、暗号化されたコンテンツと、管理センタより供給されたマスタ暗号鍵により暗号化されているコンテンツ暗号鍵と、署名と、管理センタから提供された証明書とを記録媒体に記録し、
前記復号手段提供手段は、前記復号手段に、マスタ暗号鍵と、証明書を検証するための署名用センタ公開鍵とを含め、
前記復号手段は、証明書を署名用センタ公開鍵を用いて検証することにより、コンテンツメーカの署名用コンテンツメーカ公開鍵を得て、これにより署名を検証し、証明書及び署名が共に有効であると判断した際に、前記マスタ暗号鍵により暗号化コンテンツ暗号鍵を復号し、復号したコンテンツ暗号化鍵により、コンテンツを復号し、
前記管理センタは、コンテンツメーカの署名用コンテンツメーカ公開鍵を署名用センタプライベート鍵で暗号化した情報を含む証明書と、コンテンツメーカから供給されたコンテンツ暗号鍵をマスタ暗号鍵で暗号化したデータとをコンテンツメーカに供給し、マスタ暗号鍵と署名用センタ公開鍵を前記復号手段提供手段に供給する、
ことを特徴とする請求項１に記載のディジタルコンテンツ流通方法。
【請求項４】前記復号手段は、
前記暗号化されたコンテンツ暗号鍵を復号するための情報を記憶し、この情報によりコンテンツ暗号鍵を復号し、復号したコンテンツ暗号鍵を用いて暗号化されたコンテンツを復号するＬＳＩ（大規模集積回路）と、
前記暗号化されたコンテンツ暗号鍵を復号するための情報を含み、この情報によりコンテンツ暗号鍵を復号し、復号したコンテンツ暗号鍵を用いて暗号化されたコンテンツを復号するソフトウエアと、の少なくとも一方を備える、
ことを特徴とする請求項１、２又は３に記載のディジタルコンテンツ流通方法。
【請求項５】前記コンテンツメーカは、
各コンテンツの一部を平文で記録し、他の少なくとも一部を前記コンテンツ暗号鍵により暗号化して前記記録媒体に記録する、ことを特徴とする請求項１、２、３又は４に記載のディジタルコンテンツ流通方法。
【請求項６】複数のディジタルコンテンツが記録された記録媒体であって、
コンテンツ毎に、
その少なくとも一部が、コンテンツ別の第１の暗号化鍵で暗号化されたディジタルコンテンツと、
第２の暗号化鍵により暗号化された前記第１の暗号化鍵

と、
製造者のプライベート鍵を用いて生成されたディジタル署名と、
前記製造者のディジタル署名を検証するための製造者の公開鍵を含む所定機関の証明書と、が記録されていることを特徴とするディジタルコンテンツ記録媒体。
【請求項７】各ディジタルコンテンツは、その一部が平文で、少なくとも他の一部が第１の暗号化鍵で暗号化されて記録媒体に記録されている、ことを特徴とする請求項６に記載のディジタルコンテンツ記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、著作権等で保護されるコンテンツの保護と利用の調和を取ることを可能とするディジタルコンテンツ流通方式及びディジタルコンテンツを記録した記録媒体に関する。
【０００２】
【従来の技術】ディジタル画像処理技術の進歩により、種々のコンテンツを加工・編集・複製することが可能になりつつある。しかし、コンテンツの加工・編集・複製を無秩序に認めると、著作権や肖像権が保護されなくなり、権利者の利益が損なわれてしまう。一方、これらのコンテンツの利用を制限しすぎるとコンテンツが利用されなくなる。
【０００３】これらの要件を満たすため、ディジタルすかし等の技術も提案されているが、データ処理が複雑であり、複雑なシステムが要求される。このため、データ処理技術に習熟していない利用者の立場から簡便に利用できるシステムとはなっていない。
【０００４】
【発明が解決しようとする課題】この発明は上記実状に鑑みてなされたもので、ディジタルコンテンツの利用と保護の調和を図ることを目的とする。
【０００５】
【課題を解決するための手段】上記目的を達成するため、この発明の第１の観点にかかるディジタルコンテンツ流通方法は、ディジタルコンテンツの流通を管理する管理センタ（１１）と、前記管理センタ（１１）の管理下に、ディジタルコンテンツを暗号化して流通させるコンテンツメーカ（１３）と、前記コンテンツメーカ（１３）が提供するコンテンツを復号して利用可能とする復号手段を提供する復号手段提供手段（１５，１７）と、を備える流通システムを用いてディジタルコンテンツを流通する方法であって、前記コンテンツメーカ（１３）は、コンテンツ別に生成されたコンテンツ暗号鍵（Kco）によりコンテンツを暗号化し、前記管理センタ（１１）は、暗号化されたコンテンツ暗号鍵（KPUk（Kco）；Kk（Kco））を記録媒体（２１）に記録するための情報（KPUk；Kk）をコンテンツメーカ（１３）に提供し、前記コンテンツメーカ（１３）は、コンテンツ暗号鍵（Kco）により暗号化されたコンテンツ（DC）と、暗号化されたコンテンツ暗号鍵（KPUk（Kco）；Kk（Kco））とを記録媒体（２１）に記録して流通させ、前記管理センタ（１１）は、暗号化されたコンテンツ暗号鍵（KPUk（Kco）；Kk（Kco））を復号するための復号情報（KPRk；Kk）を復号手段提供手段（１５）に提供し、前記復号手段提供手段（１５）は、前記暗号化されたコンテンツ暗号鍵を復号するための復号情報（KPRk；Kk）を前記復号手段（ＬＳＩetc）に含め、前記復号手段（ＬＳＩetc）は、前記記録媒体（２１）に記録されているコンテンツ暗号鍵（Kco）を前記復号情報（KPRk；Kk）を用いて復号し、復号した暗号鍵（Kco）で、コンテンツを復号して再生する、ことを特徴とする。
【０００６】この方法によれば、ディジタルコンテンツを暗号化した状態で流通させて不正使用を防止し、さらに、再生することができる。鍵が、管理センタを中心として三者で管理されているので信頼性及び安全性が高い。さらに、コンテンツ別に暗号化鍵が異なるので、ある暗号化鍵が破られても、それが記録媒体全体に及ぶことがなく、安全である。
【０００７】暗号化の方式として公開鍵方式を使用する場合は、次の構成が有効である。まず、前記コンテンツメーカは、コンテンツ別にコンテンツ暗号鍵を生成してコンテンツを暗号化し、生成したコンテンツ暗号鍵を管理センタから供給されたマスタ公開鍵（KPUk）により暗号化し、管理センタ（１１）から供給された署名用コンテンツメーカプライベート鍵（KPRm）を用いて自己の署名を作成し、暗号化したコンテンツと暗号化したコンテンツ暗号鍵（KPUk（Kco））と署名（ＤＳ）と管理センタ（１１）から供給された証明書（ＤＶ）とを記録媒体（２１）に格納し、前記復号手段提供手段（１５）は、前記復号手段（ＬＳＩ）に、暗号化されたコンテンツ暗号鍵（KPUk（Kco））を復号するためのマスタプライベート鍵（KPRk）と、証明書（ＤＶ）を検証するための署名用センタ公開鍵（KPUce）とを含め、前記復号手段（ＬＳＩ）は、証明書（ＤＶ）を署名用センタ公開鍵（KPUce）を用いて検証することにより、コンテンツメーカ（１３）の署名用コンテンツメーカ公開鍵（KPUm）を得て、これにより署名（ＤＳ）を検証し、証明書（ＤＶ）及び署名（ＤＳ）が共に有効であると判断した際に、前記マスタプライベート鍵（KPRk）により暗号化コンテンツ暗号鍵（KPUk（Kco））を復号し、復号したコンテンツ暗号化鍵（Kco）により、コンテンツを復号し、前記管理センタ（１１）は、マスタ公開鍵（KPUk）と、コンテンツメーカの署名用コンテンツメーカ公開鍵（KPUm）を署名用センタプライベート鍵（KPRce）で暗号化した情報（KPRce（KPUm））を含む証明書（ＤＶ）とをコンテンツメーカに供給し、マスタプライベート鍵（KPRk）と署名用センタ公開鍵

（KPUce）を前記復号手段提供手段（１５）に供給する。この方法によれば、コンテンツ暗号鍵を暗号化するための鍵と復号するための鍵が別個に管理されているので、より安全である。さらに、署名及び証明書を用いることにより、その信頼性が高い。

【０００８】暗号化の方式として秘密鍵方式を使用する場合は、次の構成が有効である。前記コンテンツメーカ（１３）は、コンテンツ別にコンテンツ暗号鍵（Kco）を生成してコンテンツを暗号化し、生成したコンテンツ暗号鍵（Kco）を管理センタ（１１）に供給し、管理センタ（１１）から供給された署名用コンテンツメーカプライベート鍵（KPRm）を用いて自己の署名（ＤＶ）を作成し、暗号化されたコンテンツ（ＤＣ）と、管理センタ（１１）より供給されたマスタ暗号鍵（Kk）により暗号化されているコンテンツ暗号鍵（Kk（Kco）と、署名（ＤＶ）と、管理センタから提供された証明書（ＤＶ）とを記録媒体（２１）に記録し、前記復号手段提供手段（１５）は、前記復号手段（ＬＳＩ）に、マスタ暗号鍵（Kk）と、証明書（ＤＶ）を検証するための署名用センタ公開鍵（KPRce）とを含め、前記復号手段（ＬＳＩ）は、証明書（ＤＶ）を署名用センタ公開鍵（KPRce）を用いて検証することにより、コンテンツメーカの署名用コンテンツメーカ公開鍵（KPUm）を得て、これにより署名（ＤＳ）を検証し、証明書（ＤＶ）及び署名（ＤＳ）が共に有効であると判断した際に、前記マスタ暗号鍵（Kk）により暗号化コンテンツ暗号鍵（Kk（Kco））を復号し、復号したコンテンツ暗号化鍵（Kco）により、コンテンツを復号し、前記管理センタ（１１）は、コンテンツメーカ（１３）の署名用コンテンツメーカ公開鍵（KPUm）を署名用センタプライベート鍵（KPRce）で暗号化した情報（KPRce（KPUm））を含む証明書（ＤＶ）と、コンテンツメーカ（１３）から供給されたコンテンツ暗号鍵（Kco）をマスタ暗号鍵（Kk）で暗号化したデータとをコンテンツメーカ（１３）に供給し、マスタ暗号鍵（Kk）と署名用センタ公開鍵（KPUce）を前記復号手段提供手段（１５）に供給する。

【０００９】この方法によれば、コンテンツ暗号鍵を暗号化するための鍵と復号するための鍵が共通であるので、復号時（再生時）の処理が高速に行うことができ、リアルタイム性が要求される用途に特に有効である。また、コンテンツ暗号化鍵を暗号化する処理がセンタで行われているため、秘密鍵方式を用いていながらその信頼性が非常に高い。さらに、署名及び証明書を用いることにより、その信頼性が高い。

【００１０】前記復号手段は、前記暗号化されたコンテンツ暗号鍵（Kco）を復号するための情報（KPRk、Kk）を記憶し、この情報によりコンテンツ暗号鍵（Kco）を復号し、復号したコンテンツ暗号鍵（Kco）を用いて暗号化されたコンテンツを復号するＬＳＩであっても、前記暗号化されたコンテンツ暗号鍵を復号するための情報を含み、この情報によりコンテンツ暗号鍵（Kco）を復号し、復号したコンテンツ暗号鍵（Kco）を用いて暗号化されたコンテンツを復号するソフトウエアであっても、よい。

【００１１】前記コンテンツメーカは、各コンテンツの一部を平文で記録し、他の少なくとも一部を前記コンテンツ暗号鍵（Kco）により暗号化して前記記録媒体に記録するようにしてもよい。このようにすれば、曲の一部、例えば、イントロを聞いて曲を確認したり、営業用に使用するさせる等の行為が容易にできる。

【００１２】上記目的を達成するため、この発明の第２の観点にかかる、複数のディジタルコンテンツが記録された記録媒体は、コンテンツ毎に、その少なくとも一部が、コンテンツ別の第１の暗号化鍵（Kco）で暗号化されたディジタルコンテンツと、第２の暗号化鍵（KPUk；Kk）により暗号化された前記第１の暗号化鍵（Kco）と、製造者のプライベート鍵を用いて生成されたディジタル署名（ＤＳ）と、前記製造者のディジタル署名を検証するための製造者の公開鍵（KPUm）を含む所定機関の証明書（ＤＶ）と、が記録されている、ことを特徴とする。

【００１３】この構成によれば、証明書を確認する情報と第１の鍵を復号する情報を有する者以外の者は、即ち、正当権限を有していない者は、所定機関の証明を確認し、さらに、その確認結果から製造者の署名を確認し、そして、コンテンツを復号することができない。従って、ディジタルデータを安全に市場に流通させることができる。

【００１４】各ディジタルコンテンツは、その一部が平文で、少なくとも他の一部が第１の暗号化鍵で暗号化されて記録媒体に記録されてもよい。

【００１５】

【発明の実施の形態】この発明の実施の形態にかかるコンテンツ流通システム及び方法を、オーディオデータ（音楽データ）を流通させる場合を例に説明する。

（第１の実施の形態）この実施の形態のコンテンツ流通システムは、図１に示すように、管理センタ１１と、コンテンツメーカ１３と、ＬＳＩ（大規模集積回路）メーカ１５と、オーディオメーカ（音響機器メーカ）１７と、ユーザ１９とを含む。

【００１６】管理センタ１１は、暗号化技術を有し、暗号化対象コンテンツの特質及び顧客の要求に応じて暗号ファイルフォーマットを設定すると共に各種暗号鍵を生成し、コンテンツメーカ１３とＬＳＩメーカ１５に供給する。管理センタ１１は、データベース１１Ａにより、顧客又は契約別に暗号ファイルフォーマット及び暗号鍵を記録して、管理する。管理センタ１１が発生する暗号鍵については図２を参照してまとめて説明する。

【００１７】コンテンツメーカ１３は、管理センタ１１の暗号ファイルフォーマットの使用許諾に基づき、コン

テンツ毎に暗号化鍵を生成してコンテンツ（ここでは、音楽データ）を暗号化し、記録媒体（例えば、フラッシュメモリ）などに格納して販売する。

【００１８】ＬＳＩメーカ１５は、管理センタ１１の暗号ファイルフォーマットの使用許諾に基づき、ＡＳＩＣ（特定用途向け集積回路）技術により、管理センタ１１が設定した暗号ファイルフォーマット及び提供された暗号鍵に従って暗号化されたコンテンツを復号する復号ＬＳＩを設計・製造し、販売する。

【００１９】復号ＬＳＩは、オーディオメーカ１７に販売される。オーディオメーカ１７は、管理センタ１１の暗号ファイルフォーマットの使用許諾に基づき、復号ＬＳＩを組み込み、コンテンツメーカ１３が提供する媒体に記録されているコンテンツデータを復号し、再生する装置（オーディオ機器）を製造し、販売する。

【００２０】管理センタ１１は、例えば、コンテンツメーカ１３，ＬＳＩメーカ１５，オーディオメーカ１７からの対価を運営資金の全部又は一部として運営される。

【００２１】ユーザ１９は、オーディオメーカ１７が提供するオーディオ機器と、コンテンツメーカ１３が提供する音楽データを格納した記録媒体とを購入し、オーディオ機器に記録媒体を装着して、音楽データを再生する。記録媒体から再生された音楽データは暗号化されたデータであるが、復号ＬＳＩにより復号され、音楽として再生される。

【００２２】次に、この流通システムで使用される各暗号鍵について図２を参照して説明する。コンテンツ鍵Ｋcoは、コンテンツメーカ１３がコンテンツ毎に乱数を発生させて生成する暗号鍵であり、流通対象のコンテンツを暗号化するためにコンテンツメーカが使用する。

【００２３】マスタ公開鍵ＫPUkは、管理センタ１１が、例えば、コンテンツメーカ毎（コンテンツ毎等でも可）に発生して供給する暗号鍵であり、供給を受けたコンテンツメーカ１３がコンテンツ鍵Ｋcoを暗号化するために使用する。

【００２４】マスタプライベート鍵 ＫPRkは、管理センタ１１が、マスタ公開鍵ＫPUkと対で発生し、各ＬＳＩメーカ１５に供給する暗号化鍵であり、復号用ＬＳＩや復号用ソフトウエアに格納され、マスタ公開鍵ＫPUkにより暗号化されたコンテンツ鍵Ｋcoを復号するために使用される。

【００２５】署名用コンテンツメーカプライベート鍵ＫPRmは、管理センタ１１がコンテンツメーカ毎に発生して提供する暗号鍵であり、コンテンツメーカが各コンテンツに署名するために使用される。

【００２６】署名用コンテンツメーカ公開鍵ＫPUmは、管理センタ１１が署名用コンテンツメーカプライベート鍵ＫPRmと対で発生し、コンテンツメーカの署名を検証するために、管理センタ１１が発行する証明書に含めて使用される。

【００２７】署名用センタプライベート鍵ＫPRceは、管理センタ１１が自ら発生し、各コンテンツメーカの署名用コンテンツメーカ公開鍵ＫPUmを暗号化して「コンテンツメーカ鍵証明書」を生成するために使用される。

【００２８】署名用センタ公開鍵ＫPUceは、管理センタ１１が、署名用センタプライベート鍵ＫPRce と対で発生する鍵であり、復号ＬＳＩに格納され、「コンテンツメーカ鍵証明書」内にある管理センタ１１の署名を検証するために使用される。

【００２９】次に、コンテンツメーカ１３が提供する音楽データについて説明する。図３に、記録媒体２１に格納される音楽データの構成例を示す。各媒体の先頭位置には、その媒体の識別コード、コンテンツメーカ１３の識別コード、媒体のタイプ、ＴＯＣ（TABLE OF CONTENTS)情報、著作権情報等の制御情報ＤＺと、Ｎ曲分の音楽のデータが記録されている。

【００３０】各曲のデータは、識別コードＤＩと、平文データＤＰと、暗号化データＤＣと、暗号化コンテンツ鍵ＤＫと、コンテンツメーカの署名ＤＳと、証明書ＤＶから構成されている。

【００３１】識別コードＤＩは、各曲の曲名、曲コード、演奏時間等を示す暗号化されていない平文データである。

【００３２】平文データＤＰは、楽曲データのうちの前半の所定時間（例えば、１０秒程度）分の暗号化されない平文データである。

【００３３】暗号化データＤＣは、楽曲データの後半の部分が、このコンテンツ用のコンテンツ鍵Ｋcoで暗号化されて生成されたデータである。

【００３４】暗号化コンテンツ鍵ＤＫは、コンテンツ鍵Ｋcoをマスタ公開鍵ＫPUkで暗号化して得られたデータＫPUk（Ｋco）である。

【００３５】コンテンツメーカの署名ＤＳは、識別コードＤＩと、平文データＤＰと、暗号化データＤＣと、暗号化コンテンツ鍵ＤＫと、をハッシュ関数等の一方向性関数Ｈ（）で変換し、これをコンテンツメーカプライベート鍵ＫPRmで暗号化して得られたデータＫPRm（Ｈ（ＤＩ；ＤＰ；ＤＣ；ＤＫ））である。

【００３６】鍵証明書ＤＶは、署名用コンテンツメーカ公開鍵ＫPUmと、この署名用コンテンツメーカ公開鍵ＫPUmを署名用センタプライベート鍵ＫPRceで暗号化して得られたデータＫPRce（ＫPUm）とを含み、コンテンツメーカが署名に使用した鍵が正当なものであることを管理センタ１１が証明するためのものである。

【００３７】次に、復号ＬＳＩについて説明する。復号ＬＳＩ３１は、図４に示すように、ドライバ３３，署名確認部３４、ＣＰＵリセット部３５、復号部３６、記憶部３７、制御部３８を備える。

【００３８】ドライバ３３は、記録媒体２１の記録データを順次読み出す。署名確認部３４は、復号対象のコン

テンツに証明書ＤＶ及び署名ＤＳが付されているか否かを判別し、付されていると判別すると、証明書ＤＶと署名ＤＳを検証する。

【００３９】即ち、署名確認部３４は、ドライバ３３が読み出した証明書ＤＶのうち、暗号化されている部分ＫPRce（KPUm）を、記憶部３７に記憶されている管理センタ１１の署名用センタ公開鍵KPUceを用いて復号して、署名用コンテンツメーカ公開鍵KPUmを得る。署名確認部３４は、復号した署名用コンテンツメーカ公開鍵KPUmと平文の署名用コンテンツメーカ公開鍵KPUmとを比較し、一致するか否かを判別する。

【００４０】一致すると判別すると、この署名用コンテンツメーカ公開鍵KPUmを用いてコンテンツメーカの署名ＤＳを検証する。即ち、署名用コンテンツメーカ公開鍵KPUmを用いて復号した署名ＤＳと、識別コードＤＩと、平文データＤＰと、暗号化データＤＣと、暗号化コンテンツ鍵ＤＫとを所定の一方向性関数Ｈ（）で変換したものが一致するか否かを判別する。署名確認部３４は、一致すると判別すると、暗号化コンテンツ鍵ＤＫ（＝KPUk（Kco））をマスタプライベート鍵KPRkを用いて復号し、コンテンツ鍵Kcoを再生する。

【００４１】ＣＰＵリセット部３５は、署名確認部３４が署名又は証明書を検出できなかった（署名又は証明書が存在しなかった）場合及び検証を認証できなかった（存在したが、認証できなかった）場合には、データの再生を禁止するため、復号ＬＳＩ３１が組み込まれている装置（再生装置）のＣＰＵ４５をリセットする。これにより、再生動作は、キャンセルされる。

【００４２】復号部３６は、署名確認部３４が署名を認証した場合に、ドライバ３３が読み出すデータを復号する部分であり、平文データについてはそのまま再生し、暗号化されているデータについては、署名確認部３４が復号したコンテンツ鍵Kcoを用いて音楽データＤＤを復号する。記憶部３７は、管理センタ１１の署名用センタ公開鍵KPUceと、コンテンツメーカ１３毎のマスタプライベート鍵KPRkとを記憶する。

【００４３】このシステムを有効に運用するためには、記憶部３７が記憶している鍵KPUceとKPRkとは厳重に秘密状態に保持する必要がある。このため、記憶部３７は、復号ＬＳＩ３１の外部から直接アクセスされないように、他の共通バスとは異なる内部バスにより署名確認部と接続されている。また、これらの鍵のデータが外部にそのまま出力されることはない。

【００４４】制御部３８は、この復号ＬＳＩ３１内の各部の動作を制御する。

【００４５】次に、この復号ＬＳＩ３１を用いたオーディオ装置の構成について説明する。図４に示すように、このオーディオ装置は、記録媒体が着脱可能に装着されるコネクタ４１と、コネクタ４１を介して記録媒体２１に接続された前述の復号ＬＳＩ３１と、復号ＬＳＩ３１から出力される音楽データをアナログデータに変換するＤ／Ａ変換器４２と、Ｄ／Ａ変換器４２の出力するアナログ信号を放音するスピーカ（ヘッドフォン等を含む）４３と、入力部４４と、このオーディオ装置全体の動作を制御するＣＰＵ（制御部）４５とから構成される。

【００４６】コネクタ４１には、記録媒体２１が着脱可能に装着される。Ｄ／Ａ変換器４２は、再生されたディジタルオーディオ信号をアナログオーディオ信号に変換して出力する。スピーカ４３は、アナログオーディオ信号を放音する。ＣＰＵ４５は、入力部４４からの入力に従って、記録媒体２１からのデータの読み出し・再生を含むこのシステム全体の動作を制御する。

【００４７】次に、この流通システムを用いたディジタルコンテンツの流通方法について説明する。音楽を記録した記録媒体２１を製造したいコンテンツメーカ１３及びその記録媒体を再生するオーディオ機器を製造したいオーディオメーカ１７は管理センタ１１に登録する。

【００４８】管理センタ１１は、コンテンツメーカ１３に暗号化フォーマットの使用を許可する場合には、暗号化フォーマットの使用を許諾し、そのノウハウを提供すると共にマスタ公開鍵KPUkと署名用プライベート鍵KPRmの対を提供する。また、証明用コンテンツメーカ公開鍵KPUmと、証明用コンテンツメーカ公開鍵KPUmを署名用センタプライベート鍵KPRceを用いて暗号化したデータKPRce（KPUm）とからなる証明書（KPUm：KPRce（KPUm））を作成し、コンテンツメーカ１３に送付する。コンテンツメーカ１３は、管理センタ１１に対し、一定のローヤリティ（対価）を支払う。

【００４９】また、管理センタ１１は、ＬＳＩメーカ１５に暗号ファイルフォーマットに準拠した復号ＬＳＩの製造を許可する場合には、その許可とノウハウを提供すると共に各コンテンツメーカのマスタプライベート鍵KPRkと自己の署名用センタ公開鍵KPUceを通知する。ＬＳＩメーカ１５は、管理センタ１１に対し、一定のローヤリティを支払う。

【００５０】また、管理センタ１１は、オーディオメーカ１７に暗号化フォーマットの使用を許可する場合には、暗号化フォーマットの使用許可を与えると共にそのノウハウを提供する。オーディオメーカ１７は、管理センタ１１に対し、一定のローヤリティを支払う。

【００５１】以下、コンテンツメーカによる記録媒体２１へのコンテンツの記録動作を図５のフローチャートを参照して説明する。まず、コンテンツメーカ１３は、例えば、記録媒体に記憶させるコンテンツ毎、即ち、楽曲毎に乱数を発生してコンテンツ鍵Kcoを生成する（ステップＳ１）。次に、その曲の識別コード、制御コードの識別データＤＩを生成する（ステップＳ２）。

【００５２】さらに、記録する楽曲の所定量の先頭部分ＤＰを平文のまま残し、残りの部分ＤＣをコンテンツ鍵Kcoで暗号化する（ステップＳ３）。ステップＳ１で生

成したコンテンツ鍵Kcoを、マスタ公開鍵KPUkで暗号化して暗号化コンテンツ鍵ＤＫを生成する（ステップＳ４）。

【００５３】さらに、上述のデータ全体、即ち、識別データＤＩと、平文データＤＰと、暗号化データＤＣと、暗号化（暗号化された）コンテンツ鍵KPUk（Kco）とを、ハッシュ関数等の一方向性関数Ｈ（）を用いて変換し、さらに、変換結果を署名用コンテンツメーカプライベート鍵KPRmで暗号化して、コンテンツメーカの署名ＤＳ（＝KPRm（Ｈ（ＤＩ；ＤＰ；ＤＣ；KPUk（Kco））））を生成する（ステップＳ５）。

【００５４】さらに、以上のデータに、管理センタ１１から提供されている証明書ＤＶを付加して（ステップＳ６）、１曲文のデータが完成する。コンテンツメーカ１３は、このようにして生成した１曲分のデータをＮ曲分適宜組み合わせて（ステップＳ７）、１記録媒体分のデータを生成し、これを記録媒体２１に記録し（ステップＳ８）、市場に流通させる（販売する）。なお、記録対象のデータを一旦メモリ上に作成すれば、そのデータを記録媒体に記録するだけで処理は完了する。

【００５５】一方、許可を受けたＬＳＩメーカ１３は、提供されたフォーマットに従って、ドライバ３３等を備える復号ＬＳＩ３１をＡＳＩＣ技術等を用いて製造する。この際、記憶部３７には、管理センタ１１の署名用センタ公開鍵KPUceと、コンテンツメーカ１３の識別コードとマスタプライベート鍵KPRkとの対を記録させる。

【００５６】許可を受けた音響オーディオメーカ１５は、ＬＳＩメーカ１５より復号ＬＳＩ３１を購入し、図４に示すような音響装置を製造する。

【００５７】オーディオメーカ１７より音響機器を購入し、コンテンツメーカ１３より記録媒体を購入したユーザ１９は、図４に示すように記録媒体２１を音響機器のコネクタ４１に装着する。

【００５８】以後、コンテンツの再生は図６のフローチャートに示すような手順で行われる。まず、入力部４４から再生の指示及びその曲番が指定されると、ＣＰＵ４５は復号ＬＳＩ３１のドライバ３３を制御してデータを読み出し、その曲の位置やコンテンツメーカの識別コードを制御情報ＤＺから判別し（ステップＳ１１）、該当記憶位置からその曲のデータ全体を読み出す（ステップＳ１２）。

【００５９】署名確認部３４は、読み出したデータから、復号（再生）対象のコンテンツに管理センタ１１の証明書ＤＶ及びコンテンツメーカ１３の署名ＤＳが付されているか否かを判別し（ステップＳ１３）、少なくとも一方が付されていないと判別すると、コンテンツの再生を防止するため、ＣＰＵリセット部３５を介してＣＰＵ４５をリセットする（ステップＳ１４）。一方、ステップＳ１３で、証明書ＤＶ及び署名ＤＳが付されていると判別すると、証明書ＤＶと署名ＤＳを検証する（ステップＳ１５～Ｓ２１）。

【００６０】即ち、署名確認部３４は、ドライバ３３が読み出した証明書ＤＶのうち、署名用コンテンツメーカ公開鍵KPUmが署名用センタプライベート鍵KPRceで暗号化されている部分KPRce（KPUm）を、記憶部３７に格納されている署名用センタ公開鍵KPUceで復号し（ステップＳ１５）、証明書ＤＶ内に平文で格納されている署名用コンテンツメーカ公開鍵KPUmと一致するか否かを判別する（ステップＳ１６）。一致しないと判別したときは、証明書ＤＶは無効であり、ＣＰＵ４５をリセットする（ステップＳ１４）。

【００６１】一方、ステップＳ１６で、一致していると判別されると、証明書ＤＶは有効であり、証明書ＤＶに含まれていた署名用コンテンツメーカ公開鍵KPUmを用いて、署名ＤＳを検証する。

【００６２】まず、署名用コンテンツメーカ公開鍵KPUmを用いて署名を復号する（ステップＳ１７）。次に、識別コードＤＩ、平文データＤＰ、暗号化データＤＣ、暗号化コンテンツ鍵ＤＫとを所定のハッシュ関数Ｈ（）で変換する（ステップＳ１８）。

【００６３】次に、ステップＳ１７で復号した内容とステップＳ１８でハッシュ関数Ｈ（）で変換したデータが一致するか否かを判別する（ステップＳ１９）。一致しなければ、署名は無効であり、ＣＰＵ４５をリセットする（ステップＳ１４）。

【００６４】ステップＳ１９で一致すると判別された場合、即ち、証明書ＤＶも署名ＤＳも有効である（暗号化鍵が正しい）と判別された場合には、署名確認部３４は、暗号化コンテンツ鍵ＤＫ（＝KPUk（Kco））を記憶部３７に格納されているそのコンテンツメーカ１３のマスタプライベート鍵KPRkを用いて復号し、コンテンツ鍵Kcoを再生する（ステップＳ２０）。

【００６５】署名確認部３４は、復号部３６に復号したコンテンツ鍵Kcoを提供すると共に復号指示信号を送出する。

【００６６】復号部３６は、復号指示信号に応答し、ドライバ３３が読み出した各曲の平文データをそのまま出力し、暗号化部分ＤＣをコンテンツ鍵Kcoを用いて復号して、出力する。この出力データはＤ／Ａ変換器４７によりアナログ信号に変換され、スピーカ４８から放音される。

【００６７】このような構成によれば、ディジタルコンテンツを暗号化して流通し、専用のＬＳＩを有する装置でのみ再生できるように構成したので、ディジタルコンテンツの不正な複製を防止することができる。また、管理センタ１１に登録するだけで、何人も実質的に共通の暗号ファイルフォーマットに準拠した製品を製造・販売することができる。さらに、コンテンツ単位で暗号化鍵が異なっているので、例え、一部の暗号化鍵が破られて

も、他の鍵が有効であり、記録媒体全体のコンテンツが盗用される自体を回避できる。

【００６８】また、記録媒体２１に記録されているデータの一部が平文で記録されているので、例えば、イントロを確認する等、音楽の一部を聞くことができる。なお、平文で記録するデータは、各楽曲の先頭部分に限定されず、各楽曲の複数箇所、ポピュラーな箇所等としてもよい。また、一部の曲については全体を平文で、他の曲については全体を暗号化して記録する等してもよい。

【００６９】なお、管理センタ１１は、この流通システムの要であり、暗号化技術に精通し、且つ、信頼及び信用の高い企業、半公的機関、公的機関が管理センタ１１の機能を実現することが望ましい。

【００７０】（第２の実施の形態）第１の実施の形態では、公開鍵暗号化方式（プライベート鍵と公開鍵の対を用いる方式）を使用したが、秘密鍵暗号方式（共通鍵方式）を使用することも可能である。以下、秘密鍵暗号方式を使用する場合の流通システムについて説明する。

【００７１】この実施の形態のコンテンツ流通システムの構成及び動作は、基本的に図１に示す第１の実施の形態の流通システムの構成及び動作と同様であり、以下の説明では、特徴部分のみを説明する。

【００７２】まず、管理センタ１１は、コンテンツメーカ１３の要請に応じて暗号ファイルフォーマットを設定すると共にコンテンツ別に暗号鍵を暗号化するためのマスタ鍵Kkを生成する。ただし、マスタ鍵Kkは、コンテンツメーカ１３にも通知されず、管理センタ１１自身で管理される。

【００７３】コンテンツメーカ１３は、乱数等を発生し、コンテンツ毎に暗号鍵（コンテンツ鍵）Kcoを生成し、各コンテンツを暗号化する。コンテンツメーカ１３は、発生したコンテンツ鍵Kcoを管理センタ１１に送付する。管理センタ１１は、送付されたコンテンツ鍵Kcoをマスタ鍵Kkで暗号化し、暗号化マスタ鍵Kk（Kco）をコンテンツメーカ１３に送付する。

【００７４】また、管理センタ１１は、証明書ＤＶに相当するデータをコンテンツメーカ１３に送付する。コンテンツメーカは、図２に示す構成と同様に、識別コードＤＩと、平文データＤＰと、暗号化データＤＣと、マスタ鍵Kkにより暗号化されたコンテンツ鍵ＤＫ（＝Kk（Kco））と、コンテンツメーカの署名ＤＳと、証明書ＤＶを組み合わせて１曲分のデータを生成し、さらに、これをＮ曲分組み合わせ、制御コードを付加して１記録媒体２５のデータを作成し、記録媒体２１に格納する。

【００７５】ＬＳＩメーカ１５は、管理センタ１１から、マスタ鍵Kkと署名用センタ公開鍵KPUceを受領し、これを記憶部３７に格納して販売する。

【００７６】このようにして、製造された記録媒体２１に記録されているコンテンツを再生する場合は、第１の実施の形態と同様に、記憶部３７に記憶されている署名用センタ公開鍵KPUceを用いて証明書ＤＶを検証し、証明書ＤＶ内に含まれている署名用コンテンツメーカ公開鍵KPUmを用いてコンテンツメーカ１３の署名ＤＳを検証する。

【００７７】検証の結果、証明書ＤＶと署名ＤＳが有効であると判断されれば、記憶部３７に記憶されているマスタ鍵Kkを用いて暗号化Ｋコンテンツ鍵ＤＫ（＝Kk（Kco））を復号してコンテンツ鍵Kcoを得て、以後、このコンテンツ鍵Kcoを用いてコンテンツを復号する。

【００７８】このような構成によれば、第１の実施の形態に比較して、より簡易な手順で、ディジタルコンテンツを暗号化して流通することができ、コストを抑え、再生時に復号に要する時間を短くすることができる。

【００７９】（実施の形態の応用例）上記第１及び第２の実施の形態では、各楽曲のデータの一部を平文で、残りの部分を暗号化して記録媒体２１に記録したが、楽曲全体を暗号化して記録してもよい。

【００８０】また、上記第１の実施の形態では、各楽曲にコンテンツメーカ１３の署名ＤＳと管理センタ１１の証明書ＤＶを付加したが、これらのデータを付加しなくてもよい。この場合は、署名ＤＳと証明書ＤＶの検証を行うことなく、コンテンツ鍵Kcoを復号し、復号されたコンテンツ鍵Kcoを用いて楽音データを復号し、再生する。

【００８１】上記実施の形態では、コンテンツを復号するために、復号ＬＳＩ３１を製造したが、ＬＳＩを製造すること自体は必ずしも必要ではなく、例えば、復号用のソフトウエアを再生装置に組み込む等してもよい。この場合は、ソフトウエアの内部に署名検証用の署名用センタ公開鍵KPUceとマスタプライベート鍵KPRk（又は、マスタ鍵Kk）を含ませておく。このような方式でも、ディジタルコンテンツを暗号化して安全に流通させ、且つ、正当権利者が再生することができる。

【００８２】上記構成では、記録媒体２１には、コントローラ（ＬＳＩ）を配置しなかったが、例えば、記録媒体２１にコントロール用のＬＳＩを配置し、認証用のデータを記録媒体２１に格納しておき、この認証用データを用いてコントローラと復号ＬＳＩ３１との間で認証処理等を行うようにしてもよい。この認証処理で、認証できない場合には、ディジタル署名が確認できなかった場合と同様にＣＰＵ４５をリセットし、再生を禁止する。

【００８３】また、この記録媒体２１のコピー回数を制限するようにしてもよい。この場合には、記録媒体２１上にコピー回数を記録する領域を配置し、コピーが行われる度にコピー回数を更新する。

【００８４】この発明は音楽データを暗号化して流通させる場合に限定されず、画像等の任意のディジタルコンテンツの流通に有効である。例えば、印刷対象の画像（例えば、ポートレートのフレームの画像等）を記録媒体に格納して流通させ、プリンタ等この記録媒体を装着

して復号ＬＳＩで再生し、印刷対象の画像と合成して印刷してもよい。

【００８５】

【発明の効果】以上説明したように、この発明によれば、任意のディジタルコンテンツの不正コピー等を防止し、ディジタルコンテンツの適切な流通を可能とする。

【図面の簡単な説明】

【図１】この発明の一実施の形態にかかるディジタルコンテンツ流通システムの基本構成を示すブロック図である。

【図２】図１に示す流通システムで使用する暗号化鍵を説明するための図である。

【図３】図１に示す流通システムで、市場に流通する記録媒体のフォーマットを示す図である。

【図４】図１に示す流通システムで、市場に流通する復号ＬＳＩ及び再生装置（オーディオ装置）の構成を示すブロック図である。

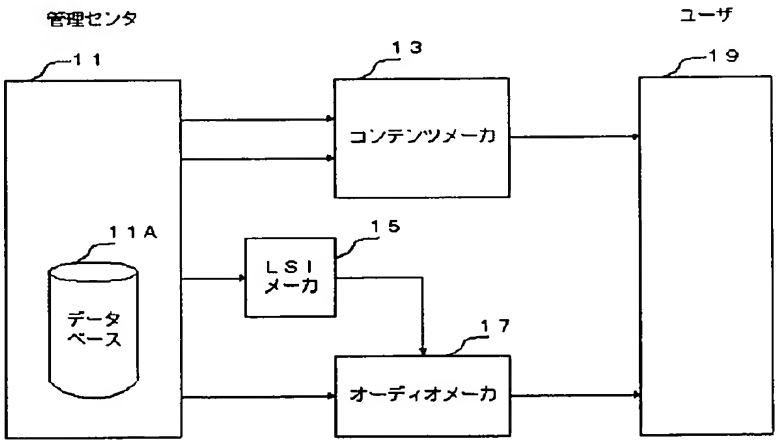
【図５】記録媒体にディジタルコンテンツを記録する処理を説明するためのフローチャートである。

【図６】記録媒体に記録されたディジタルコンテンツを再生する処理を説明するためのフローチャートである。

【符号の説明】

１１	管理センタ
１３	コンテンツメーカ
１５	ＬＳＩメーカ
１７	オーディオメーカ
１９	ユーザ
２１	記録媒体
３１	復号ＬＳＩ
３３	ドライバ
３４	署名確認部
３５	ＣＰＵリセット部
３６	復号部
３７	記憶部
３８	制御部
４１	コネクタ
４２	Ｄ／Ａ変換器
４３	スピーカ
４４	入力部
４５	ＣＰＵ

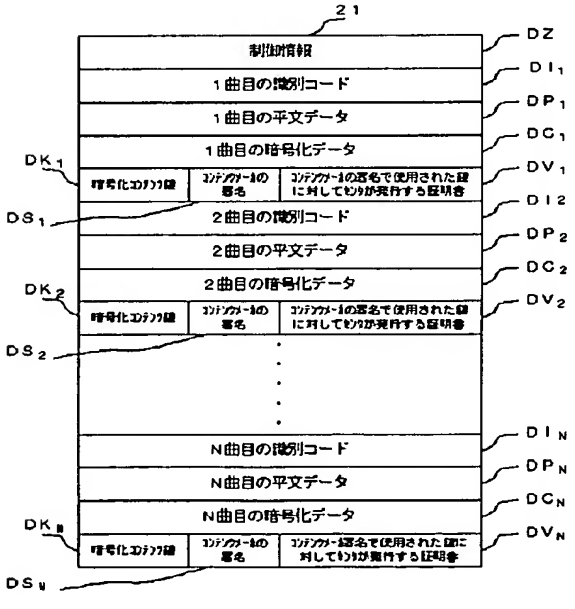
【図１】



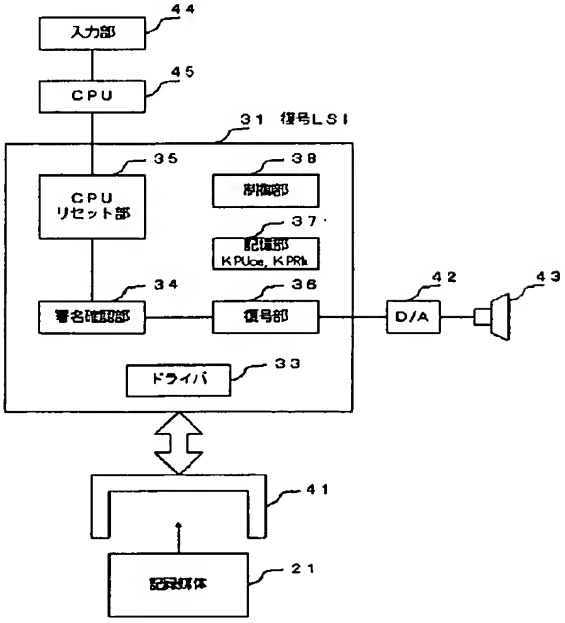
【図２】

名称	記号	発生者	内容	備考
ｺﾝﾃﾝﾂ鍵	K co	ｺﾝﾃﾝﾂﾒｰｶ	ｺﾝﾃﾝﾂを暗号化する	ｺﾝﾃﾝﾂ毎に生成される
ﾏｽﾀ公開鍵	K PUk	管理ｾﾝﾀ	ｺﾝﾃﾝﾂ鍵を暗号化する	ﾏｽﾀﾌﾟﾗｲﾍﾞｰﾄ鍵と対
ﾏｽﾀﾌﾟﾗｲﾍﾞｰﾄ鍵	K PRk	管理ｾﾝﾀ	ﾏｽﾀ公開鍵により暗号化されたｺﾝﾃﾝﾂ鍵を復号する	ﾏｽﾀ公開鍵と対
署名用ｺﾝﾃﾝﾂﾒｰｶﾌﾟﾗｲﾍﾞｰﾄ鍵	K PRm	管理ｾﾝﾀ	ｺﾝﾃﾝﾂﾒｰｶが署名を行う時に使用する	ｺﾝﾃﾝﾂﾒｰｶ毎に生成される; 署名用ｺﾝﾃﾝﾂﾒｰｶ公開鍵と対
署名用ｺﾝﾃﾝﾂﾒｰｶ公開鍵	K PUm	管理ｾﾝﾀ	ｺﾝﾃﾝﾂﾒｰｶの署名を検証する際に使用される	ｺﾝﾃﾝﾂﾒｰｶ毎に生成される; 署名用ｺﾝﾃﾝﾂﾒｰｶﾌﾟﾗｲﾍﾞｰﾄ鍵と対
署名用ｾﾝﾀﾌﾟﾗｲﾍﾞｰﾄ鍵	K PRce	管理ｾﾝﾀ	管理ｾﾝﾀがｺﾝﾃﾝﾂﾒｰｶの鍵証明書を作成する際に使用する	署名用ｾﾝﾀ公開鍵と対
署名用ｾﾝﾀ公開鍵	K PUce	管理ｾﾝﾀ	ｺﾝﾃﾝﾂﾒｰｶ鍵証明書内にあるｾﾝﾀの署名を検証する時に使用する	署名用ｾﾝﾀﾌﾟﾗｲﾍﾞｰﾄ鍵と対

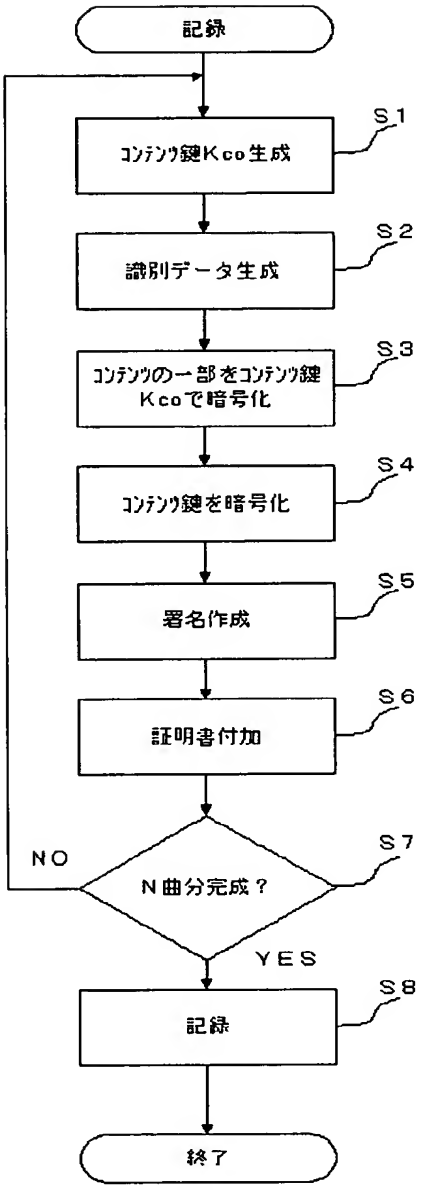
【図３】



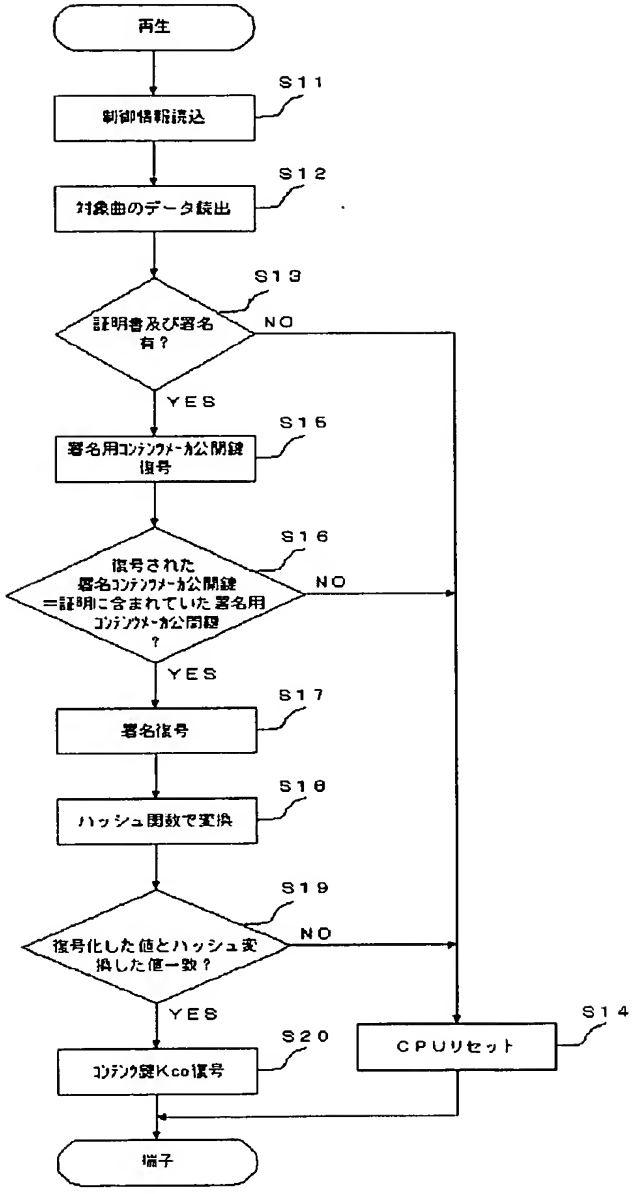
【図４】



【図５】


記録
S1
ｺﾝﾃﾝﾂ鍵Kco生成
S2
識別データ生成
S3
ｺﾝﾃﾝﾂの一部をｺﾝﾃﾝﾂ鍵Kcoで暗号化
S4
ｺﾝﾃﾝﾂ鍵を暗号化
S5
署名作成
S6
証明書付加
S7
N曲分完成？
NO
YES
S8
記録
終了

【図６】


再生
S11
制御情報読込
S12
対象曲のデータ読出
S13
証明書及び署名有？
NO
YES
S15
署名用ｺﾝﾃﾝﾂﾒｰｶ公開鍵復号
S16
復号された署名ｺﾝﾃﾝﾂﾒｰｶ公開鍵＝証明に含まれていた署名用ｺﾝﾃﾝﾂﾒｰｶ公開鍵？
NO
YES
S17
署名復号
S18
ハッシュ関数で変換
S19
復号化した値とハッシュ変換した値一致？
NO
YES
S20
ｺﾝﾃﾝﾂ鍵Kco復号
S14
CPUリセット
端子

Japanese Kokai Patent Application No. P2000-22680A

Job No.: 228-127514
Ref.: JP2003-37588 & JP2000-22680/PU030241/PPK (Fidez) ORDER NO. 159 and NO. 160
Translated from Japanese by the McElroy Translation Company
800-531-9977 customerservice@mcelroytranslation.com

(19) JAPANESE PATENT OFFICE (JP)

(12) KOKAI TOKUHYO PATENT GAZETTE (A)

(11) PATENT APPLICATION PUBLICATION NO. P2000-22680A
(43) Publication Date: January 21, 2000

(51) Int. Cl.[7]:		Identification Codes:	FI		Theme codes (reference)
H 04L	9/08		H 04 L	9/00	601 B
G 06F	15/00	330	G 06 F	15/00	330 Z
	17/60		G 09 C	1/00	620 Z
G 09C	1/00	620			640 C
		640	G 06 F	15/21	330

Examination Request: Not filed

No. of Claims: 7 (Total of 11 pages; OL)

(21) Filing No.: Hei 10[1998]-191706

(22) Filing Date: July 7, 1998

(71) Applicant: 598090519
KK Open Loop
1-18-5 Kiyota 7-jo, Kiyota-ku,
Sapporo-shi, Hokkaido

(72) Inventor: Kazunori Asada
KK Open Loop
2-5-5 Kitano 7-jo, Kiyota-ku,
Sapporo-shi, Hokkaido

(74) Agent: 100095407
Mitsuru Kimura, patent attorney and
2 others

(54) [Title] DIGITAL CONTENT DISTRIBUTION METHOD AND RECORDING MEDIUM ON WHICH CONTENT IS REPRODUCIBLY RECORDED

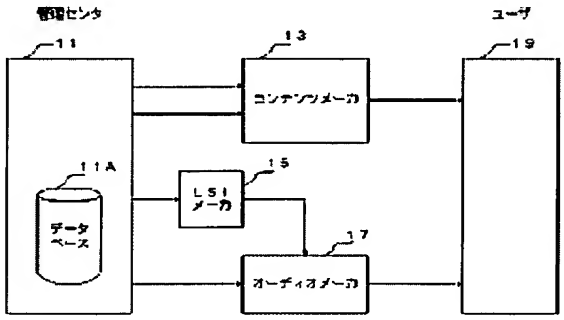
(57) Abstract

Problem

To prevent unauthorized copying and use of music or other digital content and distribute securely.

Means to solve

A management center 11 supplies a master public key KPUk to a content maker, and supplies a master private key KPRk to an LSI maker 15. Content maker 13 records data encrypted by generating a content encryption key Kco according to the content, data in which content encryption key Kco is encrypted using master public key KPUk, and a certificate DV from management center 11 on a recording medium 21. LSI maker 15 includes master private key KPRk for decoding the encrypted content encryption key in a decoding LSI. The decoder decodes the content encryption key using master private key KPRk and decodes the content using the decoding LSI, when the certificate DV and a signature DS on the mounted recording medium 21 are both determined to be valid.



Key:
- 11 Management center
- 11A Database
- 13 Content maker
- 15 LSI maker
- 17 Audio maker
- 19 User

Claims

1. A method to distribute digital content using a distribution system provided with a management center that manages the distribution of the digital content, a content maker that encrypts and distributes the digital content under the management of the aforementioned management center, and a decoding means providing means that provides a decoding means to decode and make usable the content provided by the aforementioned content maker,

the digital content distribution method being characterized in that:

the aforementioned content maker records content encrypted with a content encryption key, and an encrypted content encryption key on a recording medium and distributes the same,

the aforementioned management center provides decoding information for decoding the encrypted content encryption key to the decoding means providing means,

the aforementioned decoding means providing means includes decoding information for decoding the aforementioned encrypted content encryption key in the aforementioned decoding means,

and the aforementioned decoding means decodes the aforementioned decoding information using the content encryption key recorded on the aforementioned recording medium, and decodes and reproduces the content with the decoded encryption key.

2. The digital content distribution method described in Claim 1, characterized by the fact that:

the aforementioned content maker generates the content encryption key according to the content and encrypts the content, encrypts the generated content encryption key with a master public key supplied from the management center, creates its own signature using a content maker private key for signatures supplied from the management center, and stores the encrypted content, the encrypted content encryption key, the signature and a certificate supplied from the management center on a recording medium,

the aforementioned decoding means providing means includes a master private key for decoding the encrypted content encryption key and a center private key for signatures for authenticating the certificate in the aforementioned decoding means,

the aforementioned decoding means obtains the content maker public key for signatures for the content maker by authenticating the certificate using the center public key for signatures and authenticates the signature with that, and decodes the encrypted content encryption key with the aforementioned master private key and decodes the content with the decoded content encryption key, when the certificate and the signature are both determined to be valid,

the aforementioned management center supplies the master public key, and a certificate that includes information in which the content maker public key for signatures for the content maker is encrypted with the center private key for signatures, to the content maker, and supplies

the master private key and the center private key for signatures to the aforementioned decoding means providing means.

3. The digital content distribution method described in Claim 1, characterized by the fact that:

the aforementioned content maker generates a content encryption key according to the content and encrypts the content, supplies the generated content encryption key to the management center, creates its own signature using a content maker private key for signatures supplied from the management center, and records the content encryption key encrypted with the master encryption key supplied from the management center, the signature, and a certificate supplied from the management center on a recording medium,

the aforementioned decoding means providing means includes a master encryption key, and a center public key for signatures for authenticating the certificate in the aforementioned decoding means,

the aforementioned decoding means obtains the content maker public key for signatures for the content maker by authenticating the certificate using the center management key for signatures and authenticates the signature with that, and decodes the encrypted content encryption key with the aforementioned master encryption key and decodes the content with the decoded content encryption key, when it is determined that the certificate and the signature are both valid,

and the aforementioned management center supplies the certificate that includes information in which the content maker public key for signatures for the content maker is encrypted with the center private key for signatures, and data in which the content encryption key supplied from the content maker is encrypted with the master encryption key to the content maker, and supplies the master encryption key and the center public key for signatures to the aforementioned decoding means providing means.

4. The digital content distribution method described in Claim 1, 2 or 3, characterized by the fact that:

the aforementioned decoding means

is provided with at least an LSI (large scale integrated circuit) that stores information for decoding the aforementioned encrypted content encryption key, decodes the content encryption key using this information, and decodes the encrypted content using the decoded content encryption key,

or with software that includes information for decoding the aforementioned encrypted content encryption key, decodes the content encryption key with the information, and decodes the encrypted content using the decoded content encryption key.

5. The digital content distribution method described in Claim 1, 2, 3 or 4, characterized by the fact that:

the aforementioned content maker

records on the aforementioned recording medium a part of each content [unit] with plain text, and records at least another part encrypted with the aforementioned content encryption key.

6. A digital recording medium, which is a recording medium on which multiple digital content [units] are recorded, and which is characterized by the fact that:

for each digital content [unit],

digital content, at least a part of which is encrypted with a first encryption key according to the content,

the aforementioned first encryption key that is encrypted with a second encryption key,

a digital signature generated using a manufacturer's private key,

and a certificate for a prescribed relationship that includes a public key for the manufacturer in order to authenticate the aforementioned manufacturer's digital signature are recorded.

7. The digital content recording medium described in Claim 6, characterized by the fact that for each digital content [unit], at least a part is recorded on the recording medium with plain text, and at least another part is encrypted with the first encryption key.

Detailed explanation of the invention

[0001]

Technical field of the invention

This invention relates to a digital content distribution method and to digital content with which it is possible to achieve a balance between the protection and use of content that is protected by copyrights, etc.

[0002]

Prior art

It is becoming possible for various types of content to be processed, edited and copied due to advances in digital image processing technology. When content processing, editing and copying are haphazardly allowed, however, copyrights and portrait rights may not be protected, and benefits to the rights holder may be diminished. On the other hand, when use of the content is too restricted, the content becomes unusable.

[0003]

To satisfy these requirements, digital watermarks and other technologies have been proposed, but data processing is complicated, and a complicated system is required. For this reason, these are not considered to be systems that can be used easily from the standpoint of a user who is unfamiliar with digital processing technology.

[0004]

Problems to be solved by the invention

This invention was devised in consideration of the aforementioned situation, and has the objective of achieving balance between the use and protection of digital content.

[0005]

Means to solve the problems

In order to accomplish the aforementioned objective, the digital content distribution method pertaining to a first viewpoint of this invention is a method to distribute digital content using a distribution system provided with a management center (11) that manages the distribution of the digital content, a content maker (13) that encrypts the digital content and distributes it under the management of aforementioned management center (11), and decoding means providing means (15, 17) that provide decoding means that can decode and use the content provided by aforementioned content maker (13), and is characterized by the [following] facts. Aforementioned content maker (13) encrypts content with a content encryption key (Kco) generated according to the content. Aforementioned management center (11) provides information (KPUk; Kk) for recording the encrypted content encryption key (KPUk (Kco); Kk (Kco)) on a recording medium (21) to content maker (13). Aforementioned content maker (13) distributes content (DC) encrypted with content encryption key (Kco) and the encrypted content encryption keys (KPUk (Kco); Kk (Kco)) recorded on recording medium (21). Aforementioned management center (11) provides decoding information (KPRk; Kk) for decoding encrypted content encryption keys (KPUk (Kco); Kk (Kco)) to decoding means providing means (15). Aforementioned decoding means providing means (15) includes decoding information (KPRk; Kk) for decoding the aforementioned encrypted content encryption keys in the aforementioned decoding means (LSI etc.). Aforementioned decoding means (LSI etc.) decodes content encryption key (Kco) recorded on aforementioned recording medium (21) using aforementioned decoding information (KPRk; Kk), and decodes and reproduces the content with decoded encryption key (Kco).

[0006]

With this method, the digital content is distributed in an encrypted state to prevent unauthorized use, and in addition, it can be reproduced. The reliability and security of the keys are high, since they are managed by a third party, primarily the management center. In addition, the encryption keys differ according to the content, so even if a specific encryption key is broken, the entire recording medium will not be affected, which is secure.

[0007]

When a public key scheme is used as the encryption scheme, the following configuration is effective. First, the aforementioned content maker generates a content encryption key according to the content and encrypts the content, encrypts the generated content encryption key with a master public key (KPUk) supplied from the management center, generates its own signature using a content maker private key (KPRm) for signatures supplied from management center (11), and stores the encrypted content, encrypted content encryption key (KPUk (Kco), signature (DS) and a certificate (DV) supplied from management center (11) on recording medium (21). Aforementioned decoding means supplying means (15) includes a master private key (KPRk) for decoding encrypted content encryption key (KPUk (Kco)) and a center public key (KPUce) for signatures for authenticating certificate (DV) in aforementioned decoding means (LSI). Aforementioned decoding means (LSI) obtains a content maker public key (KPUm) for signatures for content maker (13) by authenticating certificate (DV) using center public key (KPUce) for signatures and authenticates signature (DS) with it, and decodes encrypted content encryption key (KPUk (Kco)) with aforementioned master private key (KPRk) and decodes the content with decoded content encryption key (Kco), when it is determined that certificate (DV) and signature (DS) are both valid. Aforementioned management center (11) supplies master public key (KPUk) and certificate (DV) that includes information (KPRce (KPUm) in which content maker public key (KPUm) for signatures for the content maker is encrypted with center private key (KPRce) for signatures to the content maker, and supplies master private key (KPRk) and center public key (KPUce) for signatures to aforementioned decoding means providing means (15). With this method, the key for encrypting the content encryption keys and the key for decoding are managed separately, so the method is more secure. In addition, the reliability is high due to the fact that a signature and a certificate are used.

[0008]

When a secret key scheme is used as the encryption scheme, the following configuration is effective. Aforementioned content maker (13) generates a content encryption key (Kco) according to the content and encrypts the content, supplies generated content encryption key

(Kco) to management center (11), creates its own signature (DV) [sic; (DS)] using a content maker private key (KPRm) for signatures supplied from management center (11), and records the encrypted content (DC), a content encryption key (Kk (Kco)) encrypted with a master encryption key (Kk) supplied from management center (11), signature (DV) [sic; (DS)] and a certificate (DV) supplied from the management center on recording medium (21). Aforementioned decoding means providing mean (15) includes master encryption key (Kk) and a center public key (KPRce) for signatures for authenticating certificate (DV) in aforementioned decoding means (LSI). Aforementioned decoding means (LSI) obtains a content maker public key (KPUm) for signatures for the content maker by authenticating certificate (DV) using center public key (KPRce) for signatures and authenticates signature (DS) with that, and decodes encrypted content encryption key (Kk (Kco)) with aforementioned master encryption key (Kk) and decodes the content with decoded content encryption key (Kco), when it is determined that certificate (DV) and signature (DS) are both valid. Aforementioned management center (11) supplies certificate (DV) that includes information (KPRce (KPUm)) in which content master public key (KPUm) for signatures for content maker (13) is encrypted with center private key (KPRce) for signatures, and data in which content encryption key (Kco) supplied from content maker (13) is encrypted with master encryption key (Kk) to content maker (13), and supplies master encryption key (Kk) and center public key (KPUce) for signatures to aforementioned decoding means providing means (15).

[0009]

With this method, the key for encrypting the content encryption keys and the key for decoding are the same, and processing when decoding (reproducing) can be accomplished quickly, which is particularly useful for applications where real time characteristics are required. In addition, processing to encrypt the content encryption keys is performed by the center, so the reliability is very high while a secret key scheme is used. Additionally, the reliability is high due to the fact that a signature and a certificate are used.

[0010]

The aforementioned decoding means could be an LSI that stores information (KPRk, Kk) for decoding aforementioned encrypted content encryption key (Kco), decodes content encryption key (Kco) with this information, and decodes the encrypted content using decoded content encryption key (Kco), or it could be software that includes information for decoding the aforementioned encrypted content encryption key, decoding content encryption key (Kco) with this information, and decoding the encrypted content using decoded content encryption key (Kco).

[0011]

The aforementioned content maker could also record a part of each content [unit] with plain text, and record at least another part encrypted with aforementioned content encryption key (Kco) on the aforementioned recording medium. If so, opening a part of a song, the intro for example, to identify the song, the allowance of commercial use, and other actions can easily be accomplished.

[0012]

In order to accomplish the aforementioned objective, a recording medium on which multiple digital content [units] are recorded and that pertains to a second viewpoint of this invention is characterized by the fact that, for each content [unit], digital content, at least a part of which is encrypted with a first encryption key (Kco) according to the content, aforementioned first encryption key (Kco) that is encrypted with a second encryption key (KPUk; Kk), a digital signature (DS) generated using the manufacturer's private key, and a certificate (DV) for a prescribed relationship that includes the manufacturer's public key (KPUm) for authenticating the aforementioned manufacturer's digital signature are recorded.

[0013]

With this configuration, anyone other than someone who has information to verify the certificate and information to decode the first key, that is, anyone who does not have an authorized right, is unable to verify the authenticity of the prescribed relationship, as well as verify the manufacturer's signature from the verification result and then decode the content. Therefore, it is possible for digital data to be distributed securely on the market.

[0014]

For each digital content [unit], a part could be recorded in plain text, and at least another part could be encrypted with the first encryption key.

[0015]

Embodiments of the invention

The content distribution system and method pertaining to an embodiment of this invention will be explained using a case in which audio data (music data) are distributed as a example.

First embodiment

The content distribution system in this embodiment, as shown in Figure 1, includes a management center 11, a content maker 13, an LSI (large scale integrated circuit) maker 15, an audio maker (audio device maker) 17, and a user 19.

[0016]

Management center 11 has encryption technology and sets the encrypted file format according to the properties of the content to be encrypted and customer requirements, while also generating various types of encryption keys, which are supplied to content maker 13 and LSI maker 15. Management center 11 records and manages encrypted file formats and encryption keys according to the customer or contract using a database 11A. The encryption keys generated by management center 11 will be collectively explained referring to Figure 2.

[0017]

Content maker 13 generates an encryption key for each content [unit] and encrypts the content (here, music data) based on usage permission for the encrypted file formats from management center 11, and saves them on a recording medium (a flash memory, for example), which is sold.

[0018]

LSI maker 15 designs, manufactures and sells a decoding LSI to decode the encrypted content in accordance with the encryption file format set by management center 11 and the provided encryption key, using an ASIC (integrated circuit for specific applications), based on usage permission for the encrypted file format from management center 11.

[0019]

The decoding LSI is sold to audio maker 17. Audio maker 17 incorporates the decoding LSI, based on the usage permission for the encrypted file format from management center 11, decodes the content data recorded on the medium provided by content maker 13, and manufactures and sells the reproducing device (audio device).

[0020]

Management center 11 is operated using compensation from content maker 13, LSI maker 15 and audio maker 17 as all or a part of the operating funds.

[0021]

User 19 purchases an audio device provided by audio maker 17 and a recording medium on which are stored music data provided by content maker 13, and mounts the recording medium in the audio device to reproduce the music data. The music data reproduced from the recording medium are encrypted data, and they are decoded by the decoding LSI and reproduced as music.

[0022]

Next, each of the encryption keys used with this distribution system will be explained referring to Figure 2. Content key Kco is an encryption key generated by content maker 13 generating a random number for each content [unit], and the content maker uses it for encrypting the content to be distributed.

[0023]

Master public key KPUk is an encryption key generated and supplied by management center 11 for each content maker (can also be for each content [unit], etc.), and is used by content maker 13 to which it is supplied to encrypt content key Kco.

[0024]

Master private key KPRk is an encryption key generated by management center 11 and paired with master public key KPUk, and is supplied to each LSI maker 15. It is stored in the decoding LSI or in decoding software, and is used for decoding content key Kco that has been encrypted with master public key KPUk.

[0025]

Content maker private key KPRm for signatures is an encryption key generated and provided by management center 11 for each content maker. It is used for the content maker to sign each content [unit].

[0026]

Content maker public key KPUm for signatures is generated by management center 11 and paired with content maker private key KPRm for signatures. It is used while included in a certificate issued by management center 11 in order to authenticate the content maker signature.

[0027]

Center private key KPRce for signatures is generated independently by management center 11, and is used to encrypt content maker public key KPUm for signatures for each content maker and generate a "content maker key certificate."

[0028]

Center public key KPUce for signatures is a key generated by management center 11 and paired with center private key KPRce for signatures. It is stored in the decoding LSI and is used to authenticate the signature of management center 11 within the "content maker key certificate."

[0029]

Next, the music data provided by content maker 13 will be explained. An example of the music data stored on recording medium 21 is shown in Figure 3. At the beginning position on each medium, the medium's identification code, an identification code for content maker 13, the medium type, TOC (TABLE OF CONTENTS) information, control information DZ, such as copyright information, and data for N songs' worth of music are recorded.

[0030]

The data for each song are configured from an identification code DI, plain text data DP, encrypted data DC, encrypted content key DK, content maker signature DS, and certificate DV.

[0031]

Identification code DI consists of non-encrypted plain text data that indicate the name, song code, performance time, etc. of each song.

[0032]

Plain text data DP consist of non-encrypted plain text data for a prescribed time (around 10 sec, for example) in the first half of the song data.

[0033]

Encrypted data DC are data generated by encrypting the last half portion of the song data with content key Kco for the content.

[0034]

Encrypted content key DK consists of data KPUk (Kco) obtained by encrypting content key Kco with master public key KPUk.

[0035]

Content maker signature DS consists of data KPRm (H (DI; DP; DC; DK)) obtained by converting identification code DI, plain text data DP, encrypted data DC, and encrypted content key DK with a hash function or another one-way function H() and encrypting this with content maker private key KPRm.

[0036]

Key certificate DV includes content maker public key KPUm for signatures, and data KPRce (KPUm) obtained by encrypting content maker public key KPUm for signatures with center private key KPRce for signatures, and is for the purpose of management center 11 certifying that the key used by the content maker for the signature is valid.

[0037]

Next, the decoding LSI will be explained. Decoding LSI 31, as shown in Figure 4, is provided with a driver 33, a signature verification unit 34, a CPU reset unit 35, a decoding unit 36, a storage unit 37, and a control unit 38.

[0038]

Driver 33 successively reads the recorded data on recording medium 21. Signature verification unit 34 determines whether certificate DV and signature DS have been attached to the content to be decoded, and authenticates certificate DV and signature DS when it is determined that they attached.

[0039]

Specifically, signature verification unit 34 decodes portion KPRce (KPUm) that is encrypted within certificate DV read by driver 33 using center public key KPUce for signatures from management center 11 stored in storage unit 37, and obtains content maker public key KPUm for signatures. Signature verification unit 34 compares decoded content maker public key KPUm for signatures and the plain-text content maker public key KPUm for signatures and determines whether they match.

[0040]

When it is determined that they match, content maker signature DS is authenticated using content maker public key KPUm for signatures. Specifically, whether signature DS decoded using content maker public key KPUm for signatures, identification code DI, plain text data DP,

encrypted data DC and encrypted content key DK converted with a prescribed one-way function H() match is determined. When signature verification unit 34 determines that they match, encrypted content key DK (=KPUk (Kco)) is decoded using master private key KPRk, and content key Kco is reproduced.

[0041]

CPU reset unit 35 resets CPU 45 of the device in which decoding LSI 31 is incorporated (reproducing device) to prohibit data reproduction when signature verification unit 34 cannot detect a signature or certificate (no signature or certificate is present) and when authentication cannot be certified (present, but cannot be certified). The reproduction operation is canceled by this.

[0042]

Decoding unit 36 is the portion that decodes the data read by driver 33 when signature verification unit 34 certifies the signature, and reproduces the plain text data without changes and decodes music data DD for the encrypted data using content key Kco decoded by signature verification unit 34. Storage unit 37 stores center public key KPUce for signatures for management center 11 and a master private key KPRk for each content maker 13.

[0043]

In order for the system to be operated effectively, it is necessary for keys KPUce and KPRk stored by storage unit 37 to be kept strictly secret. For this reason, storage unit 37 is connected to the signature verification unit using an internal bus that is different from the other common buses so as not to be directly accessible from outside decoding LSI 31. Data for the keys are also not output unchanged to the outside.

[0044]

Control unit 38 controls the operation of each unit in decoding LSI 31.

[0045]

Next, the configuration of the audio device that uses decoding LSI 31 will be explained. As shown in Figure 4, the audio device is configured with a connector 41 where the recording medium can be detachably mounted, aforementioned decoding LSI 31 that is connected to recording medium 21 through connector 41, a D/A converter 42 that converts the music data output from decoding LSI 31 to analog data, a speaker (including headphones, etc.) 43 that

produces sound from the analog signals output by D/A converter 42, an input unit 44, and a CPU (control unit) 45 that controls all operations of the audio device.

[0046]

Recording medium 21 is detachably mounted in connector 41. D/A converter 42 converts the reproduced digital audio signal to an analog audio signal and outputs it. Speaker 43 produces sound from the analog audio signal. CPU 45 controls all operations of the system, including the reading and reproduction of data from recording medium 21, in accordance with input from input unit 44.

[0047]

Next, a digital content distribution method that uses the distribution system will be explained. Content maker 13 that wants to manufacture recording media 21 on which music is recorded, and audio maker 17 that wants to manufacture audio devices to play the recording media are registered at management center 11.

[0048]

When use of the encrypted file format is permitted for a content maker 13, management center 11 permits use of the encrypted file format, provides the knowhow for this, and also provides the paired master public key KPUk and private key KPRm for signatures. A certificate (KPUm: KPRce (KPUm)) comprising content maker public key KPUm for certification and data KPRce (KPUm) in which content maker public key KPUm for certification is encrypted using center private key KPRce for signatures is created and is sent to content maker 13. Content maker 13 pays a fixed royalty (compensation) to management center 11.

[0049]

When manufacture of a decoding LSI conforming to the encrypted file format is permitted for an LSI maker 15, management center 11 provides the permission and the knowhow, and also notifies the master private key KPRk for each content maker and center public key KPUce for its own signature. LSI maker 15 pays a fixed royalty to management center 11.

[0050]

In addition, when use of the encrypted file format is permitted for an audio maker 17, management center 11 gives permission to use the encrypted file format and also provides the knowhow for it. Audio maker 17 pays a fixed royalty to management center 11.

[0051]

The operation of recording content to recording medium 21 by a content maker will be explained below referring to the flow chart in Figure 5. First, content maker 13 generates a random number for each content [unit], that is, each song, stored on the recording medium, for example, and generates a content key Kco (step S1). Next, song identification code and control code identification data DI are generated (step S2).

[0052]

Additionally, a prescribed amount of the beginning portion DP of the songs to be recorded is left as plain text, and the remaining portion DC is encrypted with content key Kco (step S3). Content key Kco generated at step S1 is encrypted with master public key KPUk and encrypted content key DK is generated (step S4).

[0053]

Additionally, all of the abovementioned data, that is, identification data DI, plain text data DP, encrypted data DC, and encrypted (that has been encrypted) content key KPUk (Kco) are converted using a hash function or another one-way function H(). The conversion result is additionally encrypted with content maker private key KPRm for signatures, and a content maker signature (=KPRM (H (DI; DP; DC; KPUk (Kco))) is generated (step S5).

[0054]

Certificate DV provided from management center 11 is additionally added to the data above (step S6), and the data for 1 song are complete. Content maker 13 combines data for 1 song that are generated in this way are combined in N songs' worth as appropriate (step S7), data for 1 recording medium are generated, they are recorded on recording medium 21 (step S8), and [the medium] is distributed on the market (sold). Note that once the data to be recorded are created in memory, processing is finished just by the data being recorded on the recording medium.

[0055]

At the same time, LSI maker 13 [sic; 15] that has received permission manufactures a decoding LSI 31 provided with driver 33, etc. in accordance with the provided format using ASIC technology, etc. In this instance, center public key KPUce for signatures for management center 11, and the pair of identification code and master private key KPRk for content maker 13 are recorded in storage unit 37.

[0056]

Audio maker 15 [sic; 17] that has received permission purchases decoding LSI 31 from LSI maker 15 and manufactures an audio device as shown in Figure 4.

[0057]

A user 19 who purchases an audio device from audio maker 17 and a recording medium from content maker 13 mounts recording medium 21 in connector 41 of the audio device as shown in Figure 4.

[0058]

Next, content reproduction is performed with the steps shown in the flow chart in Figure 6. First, when reproduction is instructed and a song number is designated from input unit 44, CPU 45 controls driver 33 of decoding LSI 31 and data are read, the song's position and the content maker identification code are identified from control information DZ (step S11), and all the data for the song are read from the relevant storage position (step S12).

[0059]

Signature confirmation unit 34 determines whether certificate DV for management center 11 and signature DS for content maker 13 have been attached to the content to be decoded (reproduced) (step S13). When it is determined that at least one has not been attached, CPU 45 is reset through CPU reset unit 35 in order to prevent content reproduction (step S14). On the other hand, when it is determined at step S13 that certificate DV and signature DS have been attached, certificate DV and signature DS are authenticated (steps S15-S21).

[0060]

Specifically, signature verification unit 34 decodes the portion KPRce (KPUm), where content maker public key KPUm for signatures that is encrypted with center private key KPRce for signatures, within certificate DV read by driver 33, with center public key KPUce for signatures that is saved in storage unit 37 (step S15), and determines whether it matches the content maker public key KPUm for signatures saved with plain text in certificate DV (step S16). When it is determined that they do not match, certificate DV is invalid, and CPU 45 is reset (step S14).

[0061]

On the other hand, when it is determined at step S16 that they do match, certificate DV is valid, and signature DS is authenticated using content maker public key KPUm for signatures included in certificate DV.

[0062]

First, the signature is decoded using content maker public key KPUm for signatures (step S17). Next, identification code DI, plain text data DP, encrypted data DC, and encrypted content key DK are converted with prescribed hash function H() (step S18).

[0063]

Next, whether the content decoded at step S17 and the data converted with hash function H() at step S18 match is determined (step S19). If they do not match, the signature is invalid, and CPU 45 is reset (step S14).

[0064]

When it is determined at step S19 that they do match, that is, that both certificate DV and signature D are valid (the encryption key is correct), signature verification unit 34 decodes encrypted content key DK (= KPUk (Kco)) using master private key KPRk for content maker 13 that was saved in storage unit 37, and content key Kco is reproduced (step S20).

[0065]

Signature verification unit 34 provides decoded content key Kco to decoding unit 36 and also outputs a decode instruction signal.

[0066]

Decoding unit 36 responds to the decode instruction signal, outputs the plain text data for each song read by driver 33 without change, and decodes encrypted portion DC using content key Kco and outputs it. The output data are converted to an analog signal by D/A converter 47, and sound is produced from speaker 48.

[0067]

With such a configuration, digital content is encrypted and distributed, and can be reproduced only with a device that has a specialized LSI, so unauthorized copying of the digital content can be prevented. In addition, it is possible for essentially anyone to manufacture/sell products that conform to the common encrypted file format just by registering at management

center 11. Additionally, the encryption keys differ by content units, so even if some of the encryption keys are broken, the other keys are valid, and a thing itself [sic; situation] where the content of the entire recording medium will be pirated can be avoided.

[0068]

In addition, a part of the data recorded on recording medium 21 is recorded with plain text, so a part of the music can be heard, for example, the intro can be verified. Note that the data recorded with plain text are not limited to the beginning portion of the individual songs, but could also be multiple locations within each song, popular locations, etc. In addition, some of the songs could be completely recorded with plain text, and the other songs could be completely encrypted.

[0069]

Note that management center 11 is required for this distribution system, and it is preferable that businesses, semi-public institutions and public institutions that are conversant in encryption technology, and that are highly reliable and trustworthy, realize the functions of management center 11.

[0070]

Second embodiment

With the first embodiment, a public key encryption scheme (scheme using a pair of a private key and a public key) was used, but a secret key encryption scheme (common key scheme) can also be used. A distribution system in which a secret key encryption scheme is used will be explained below.

[0071]

The configuration and operation of the content distribution system in this embodiment are basically the same as the configuration and operation of the distribution system in the first embodiment shown in Figure 1, and in the explanation below, only the distinctive portions will be explained.

[0072]

First, management center 11 sets the encrypted file format according to a request by content maker 13 and also generates master key Kk for encrypting the encryption key according to the content. Here, content maker 13 is not notified of master key Kk and is managed by management center 11.

[0073]

Content maker 13 generates random numbers, generates encryption key (content key) Kco for each content [unit], and encrypts each content [unit]. Content maker 13 sends the generated content key Kco to management center 11. Management center 11 encrypts the content key Kco that was sent with master key Kk and sends encrypted master key Kk (Kco) to content maker 13.

[0074]

Management center 11 also sends data corresponding to certificate DV to content maker 13. The content maker generates data for 1 song by combining identification code DI, plain text data DP, encrypted data DC, content key DK encrypted with master key Kk (=Kk (Kco)), content maker signature DS, and certificate DV, identical to the configuration shown in Figure 2, and additionally combines N songs' worth of this, adds controls codes to generate data for 1 recording medium 25, and saves on recording medium 21.

[0075]

LSI maker 15 receives master key Kk and center public key KPUce for signatures from management center 11 and saves them in storage unit 37, which is sold.

[0076]

When content recorded on recording medium 21 that is manufactured in this way is reproduced, certificate DV is authenticated using center public key KPUce for signatures stored in storage unit 37, and signature DS of content maker 13 is authenticated using content maker public key KPUm included in certificate DV, in the same way as in the first embodiment.

[0077]

If as a result of authentication, it is determined that certificate DV and signature DS are valid, encrypted K [sic] content key DK (= Kk (Kco)) is decoded using master key Kk stored in storage unit 37 to obtain content key Kco, and the content is decoded thereafter using content key Kco.

[0078]

With such a configuration, digital content can be encrypted and distributed with a simpler procedure, costs can be held down, and the time required for decoding when reproducing can be shortened, in comparison with the first embodiment.

[0079]

Application examples of the embodiments

With the first and second embodiments above, a part of the data for each song is recorded on recording medium 21 with plain text, and the remaining portion is encrypted, but all of the songs could also be encrypted and recorded.

[0080]

In addition, with the first embodiment above, signature DS of content maker 13 and certificate DV for management center 11 are added to each song, but these data need not be added. In this case, content key Kco is decoded and the music data are decoded and reproduced using decoded content key Kco without authenticating signature DS and certificate DV.

[0081]

With the embodiments above, decoding LSI 31 was manufactured to decode the content, but the manufacture of said LSI is not necessarily required. For example, software for decoding could be incorporated into the reproducing device. In this case, center public key KPUce for signatures for signature authentication and master private key KPRk (or master key Kk) are included in the software. With such a scheme as well, digital content can be encrypted and securely distributed, and valid rights holders can reproduce it.

[0082]

With the configuration above, a controller (LSI) was installed for recording medium 21, but, for example, an LSI for control could be installed on recording medium 21, data for verification could be saved on recording medium 21, and verification processing could be carried out between the controller and decoding LSI 31. When verification is not possible with this verification processing, CPU 45 is reset and reproduction is prohibited, as in the case when a digital signature cannot be verified.

[0083]

The number of times recording medium 21 is copied could also be restricted. In this case, a region to record the number of copies is placed on recording medium 21, and the number of copies is updated each time copying is performed.

[0084]

This invention is not limited to cases where music data are encrypted and distributed and is effective for distribution of any digital content, such as images. For example, images to be printed (portrait frame images, for example) could be saved on a recording medium and distributed, and the recording medium could be mounted in a printer or the like and reproduced with a decoding LSI, and printing could be accomplished in combination with the images to be printed.

[0085]

Effect of the invention

As explained above, with this invention, unauthorized copying, etc. of any digital content can be prevented, and appropriate distribution of digital content is enabled.

Brief description of the figures

Figure 1 is a block diagram showing the basic configuration of a digital content distribution system pertaining to one embodiment of this invention.

Figure 2 is a figure for explaining the encryption keys used with the distribution system shown in Figure 1.

Figure 3 is a figure for explaining the format of a commercially distributed recording medium distributed, with the distribution system shown in Figure 1.

Figure 4 is a block diagram showing the configuration of the decoding LSI and a commercially distributed reproducing device (audio device), with the distribution system shown in Figure 1.

Figure 5 is a flow chart for explaining processing to record the digital content on the recording medium.

Figure 6 is a flow chart for explaining processing to reproduce the digital content recorded on the recording medium.

Explanation of symbols

11 Management center
13 Content maker
15 LSI maker
17 Audio maker
19 User
21 Recording medium
31 Decoding LSI

33 Driver
34 Signature verification unit
35 CPU reset unit
36 Decoding unit
37 Storage unit
38 Control unit
41 Connector
42 D/A converter
43 Speaker
44 Input unit
45 CPU

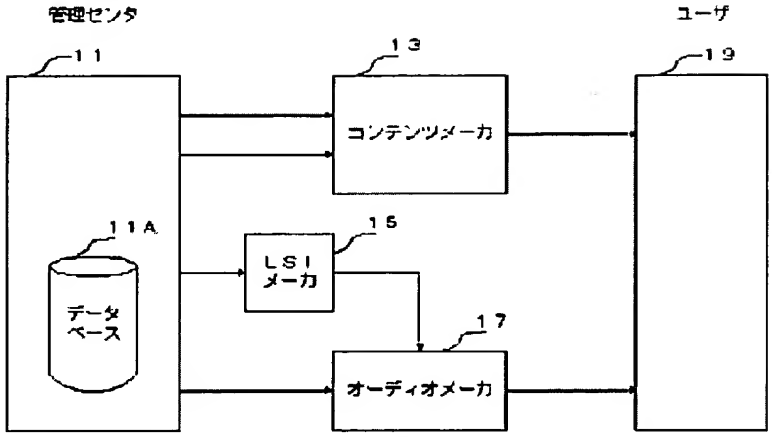


Figure 1

Key: 11 Management center
11A Database
13 Content maker
15 LSI maker
17 Audio maker
19 User

Name	Code	Originator	Content	Remarks
Content key	K co	Content maker	Encrypts content	Generated for each content [unit]
Master public key	K PUk	Management center	Encrypts content key	Paired with master private key
Master private key	K PRk	Management center	Decodes content key encrypted with master public key	Paired with master public key
Content maker private key for signatures	K PRm	Management center	Used when content maker performs [sic; creates] signatures	Generated for each content maker; paired with content maker public key for signatures
Content maker public key for signatures	K PUm	Management center	Used when content maker signature is authenticated	Generated for each content maker; paired with content maker private key for signatures
Center private key for signatures	K PRce	Management center	Used when management center creates key certificate for content maker	Paired with center public key for signatures
Center public key for signatures	K PUce	Management center	Used when content maker authenticates center signature in key certificate	Paired with center private key for signatures

Figure 2

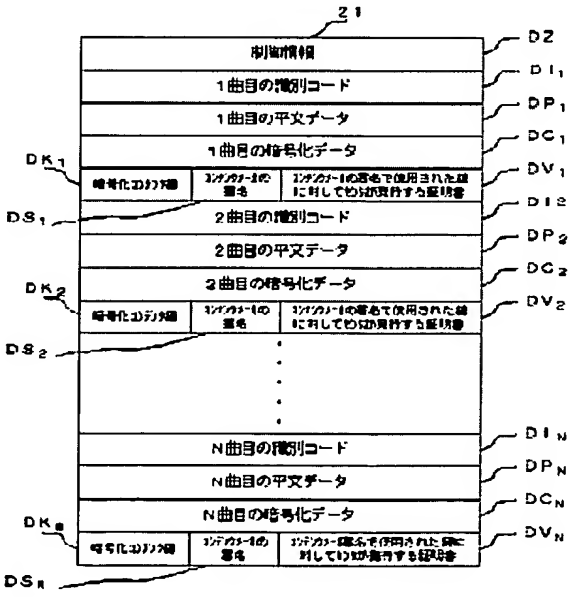


Figure 3

Key: DZ Control information
DI_1 First song identification code
DP_1 First song plain text data
DC_1 First song encrypted data
DK_1 Encrypted content key
DS_1 Content maker's signature
DV_1 Certificate issued by center for key used with content maker's signature
DI_2 Second song identification code
DP_2 Second song plain text data
DC_2 Second song encrypted data
DK_2 Encrypted content key
DS_2 Content maker's signature
DV_2 Certificate issued by center for key used with content maker's signature
DI_N Nth song identification code
DP_N Nth song plain text data
DC_N Nth song encrypted data
DK_N Encrypted content key
DS_N Content maker's signature
DV_N Certificate issued by center for key used with content maker's signature

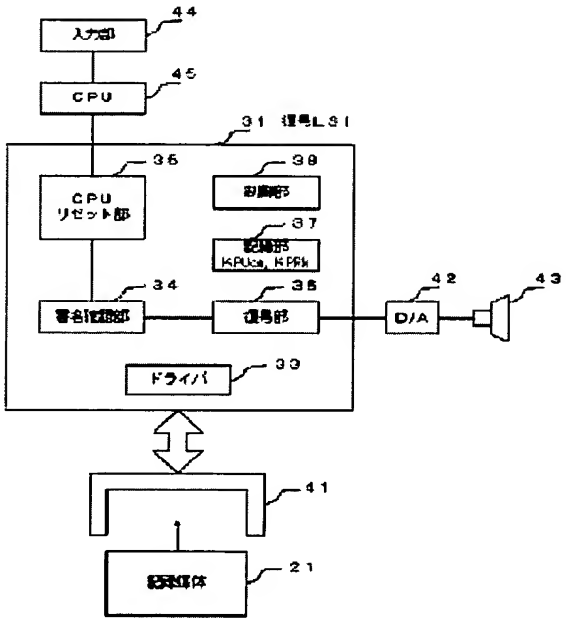


Figure 4

Key: 21 Recording medium
31 Decoding LSI

33 Driver
34 Signature verification unit
35 CPU reset unit
36 Decoding unit
37 Storage unit
38 Control unit
44 Input unit

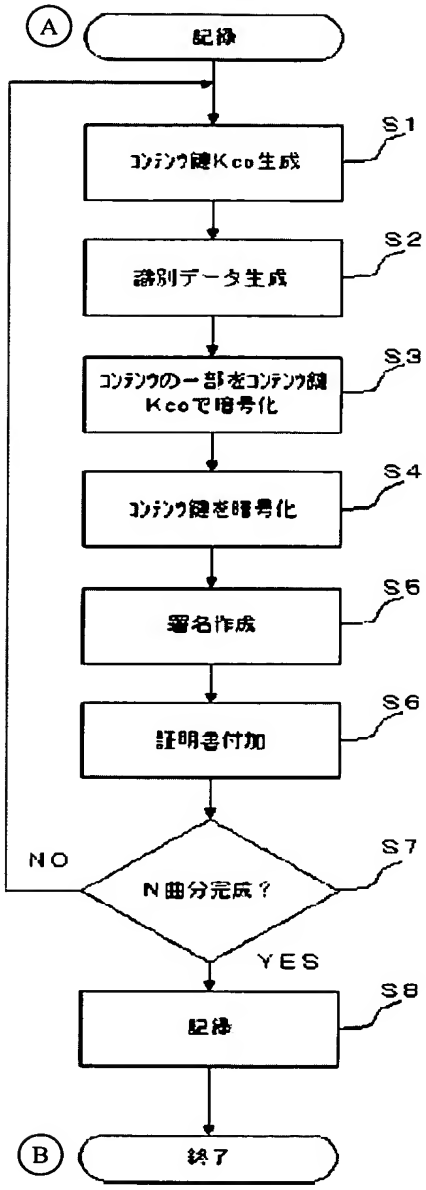


Figure 5

Key:
- A Recording
- B End
- S1 Content key Kco generation
- S2 Identification data generation
- S3 Part of content is encrypted with content key Kco
- S4 Content key is encrypted

S5 Signature creation
S6 Certificate addition
S7 N songs' worth complete?
S8 Recording

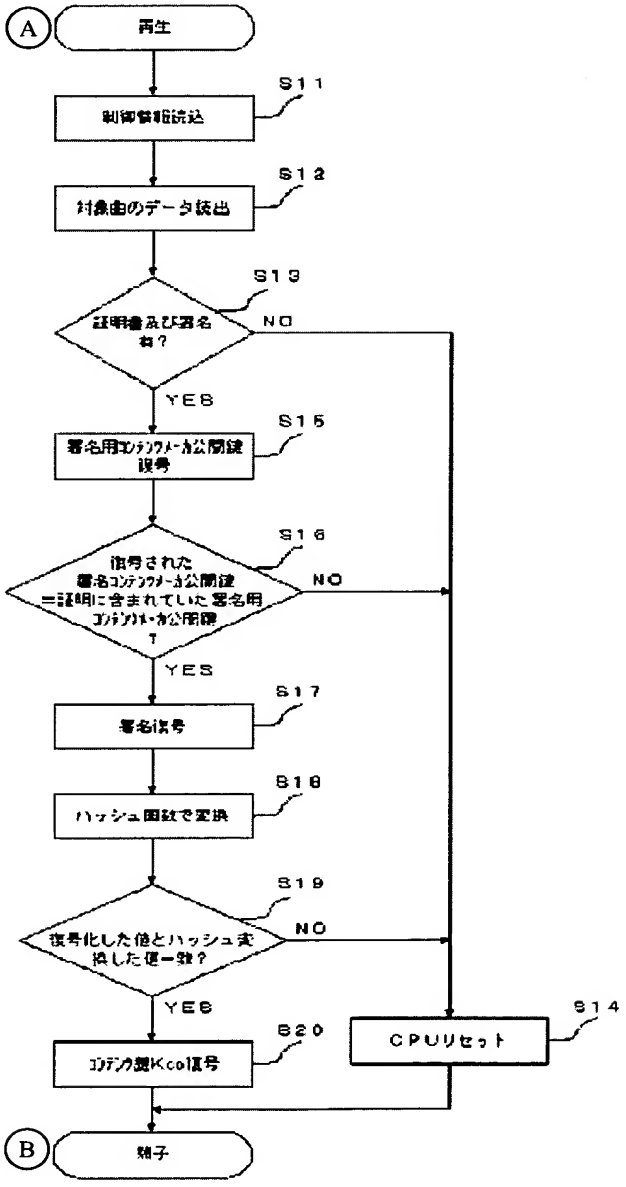


Figure 6

Key: A Reproduction
B Terminal [sic; End]

S11 Reading in of control information
S12 Reading of target song data
S13 Certificate and signature present?
S14 CPU reset
S15 Encryption of content maker public key for signatures
S16 Decoded content maker public key [for] signatures = content maker public key for signatures included in certificate?
S17 Signature decoding
S18 Conversion with hash function
S19 Do decoded value and hash converted value match?
S20 Decoding of content key Kco